Authentication

Definition: is the process of verifying the identity user

Or a technical action that prevents unauthorized people or unauthorized processes form entering a computer system

ازاي اتعرف علي هويه اليوزر اللي داخل عندي علي السيستم او امنع اي يوزر او عمليه معينه مش موثوق فيهم من الدخول علي السيستم.

Authentication challenge

في بعض التحديات اللي بتقابلني في عمليه Authentication وهي

١) تجميع الداتا بتاعت Authentication
٢) ازاي ابعت الداتا دي بامان يعني مفيش هكر يقدر يخش ويعرف الداتا دي
٣) ازاي اعرف ان الشخص اللي هابعتله الداتا دي لسه الشخص اللي بيستخدم السيستم مش حد تاني جه مكانه يعني لو مستخدم جهاز وعملت لوجن عليه وقمت وجه واحد تاني استخدم الجهاز ده المفروض مايعرفش يستخدم البيانات دي او يستخدم السيستم

Authentication Mechanism

1) **Something you know** زي اليوزرنيم و الباسورد كده

مميزات الباسورد انه كويس للسيكيورتي علي المدي البعيد وموجود في كل الانظمه يعني مالوف بالنسبه لليوزر

عيوب الباسورد انه ممكن يتنسي او يتخمن او حد يشوفك وانت بتكتبه فيحفظه او لو موجود في ملف حد يعرف الملف ده ويستخدم الباسورد في الدخول للسيستم ولو موحد الباسورد لكل المواقع او الانظمه هاتبقي مشكله كبيره اوي

2) **Something you have** زي مفتاح او كارت

برده زي كارت ATM لازم باسورد وبدخل الكارت وبيشوف هل انت اليوزر اللي عنده ولا لا

عشان اخلي النظام ده اقوي اعمله مع النظام اللي قبله something you know ومعظم الانواع في النوع ده بتنقسم الي نوعين memory token and smart token

Memory token

عباره عن خليط من حاجه اليوزر عارفها زي الباسورد و حاجه اليوزر معاه زي الكارت

مميزاتها انها بتزود السيكيورتي عن الباسورد لما يبقي لوحده ومش غاليه وعشان حد يخترق السيستم لازم يعرف الباسورد ويكون معاه الكارت

عيبوبها انها ممكن تضيع او اليوزر ميستريحلهاش بتحتاج reader عشان يقدر يقرا الكارت وده بيبقي غالي وبيزود التكلفه و pins اللي بتبقي فيها معرضه للتلف فحمايتها بتبقي صعبه شوية

Smart token

ودي من امثله memory token وبيبقي فيها اكتر من IC وبتبقي عن طريق الباسورد والكارت كمان وبتتكون من

- **Physical characteristic**

ودي الكارت نفسه وبيحتوي علي **مايكروبروسيسور**

Smart token that are not smart cards can look like calculator, key, or other small portable object

- **Interface**

ودي الواجهه وبتبقي يا اما manual او electronic interface

ودي لوحه مفاتيح بتسمح لليوزر انه يتصل بالكارت ويبادل المعلومات معاه Manual

هو اللي بيقرا الكارت لوحده Electronic interface

- **Protocol used**

الطريقه اللي بتتم بيها عمليه authentication وبتبقي ٣ انواع

- عن طريق باسورد ثابت
- او عن طريق باسورد متغير يعني جهاز بيولد باسوردات كل مرة استخدمه
- او عن طريق challenge response يعني جهاز بيستخدم عشان يولد challenge ارقام عشوائيه و smart token بتولد response بناء علي challenge ده والبروتوكول ده مبني علي cryptography وممكن يستخدم يا اما manual او electronic interface

مميزات smart token

انها بتقدم flexibility عاليه وسيكيورتي عاليه عن الانواع اللي قبل كده وحلت مشاكل authentication منها ان لو حد شاف الباسورد مايقدرش يعمل بيه حاجه

عيوب smart token

تكلفتها عاليه وممكن pins يحصلها حاجه وادارتها صعبه لانها بتتحكم في الباسورد و memory token

3) **Something you are** زي البيومترك بالبصمه او الصوت

وبتنقسم لنوعين physical و behavioral

Physical زي البصمه او شبكيه العين و behavioral زي الصوت والامضاء

مميزاتها ان السيكيورتي عاليه جدا وصعب اوي انها تخترق

عيوبها انها معقده و غاليه وممكن اليوزر اللي هايستخدموها مايتقبلوهاش

Authentication Procedures:

1) Two parity authentication scheme
2) Third parity authentication scheme
3) Public key authentication process

Two parity authentication scheme

1. Own way authentication

Client بيعرف نفسه لل server

اليوزر بيطلب اليوزرنيم والباسورد من السيرفر والوالسيرفر بيبعتهمله وبيتاكد ان مفيش حد تاني مستخدم اليوزرنيم والباسورد ده

2. Two way authentication

هنا client و server بيعرفوا بعض

Both parties authenticated to each other

اليوزر بيطلب اليوزرنيم والباسورد من السيرفر والوالسيرفر بيبعتهمله وبيتاكد ان مفيش حد تاني مستخدم اليوزرنيم والباسورد ده وبعد كده السيرفر بيعرف نفسه لل client وبيبعتله اسمه والباس بتاعه متشفر وبعد كده لازم client يتاكد ان مفيش سيرفر تاني عنده الباسورد ده

بس الطريقه دي فيها بعض المشاكل اللي بتخليها ماتستخدمش

نتخيل كده لو عندي شبكه فيها خمسين جهاز وكل جهاز فيهم عايز يكلم الجهاز التاني يبقي لازم الجهاز ده يكون متعرف علي الاجهزه التانيه ولاسباب السيكيورتي لازم الباسوردات بتاعت الاجهزه دي تبقي متخزنه عنده فالنتيجه كده ان كل جهاز هايخزن 49 باسورد

Inefficient technique

Third parity authentication scheme

يعتبر امتداد لل two party بيزود عليه انه ممكن يخزن الباسوردات ويعملها maintenance

مابيبيعتش الباسوردات علي النت بيخزنهم عنده في سيرفر واي يوزر لما بيدخل علي النظام بيبقي لمده معينه ومن امثلته

KERBEROS

Two way third party authentication

Symmetric key with Key distribution center (KDC) known as Kerberos server

لما بيطلب اليوزر والباس بيطلب معاه ticket ودي بيبقي فيها المده اللي هايفضل مستخدم فيها السيستم ودي ليها سيرفر خاص بيها في Kerberos server

Kerberos information Exchange

بيتم تبادل المعلومات في السيرفر

1) Client authentication server exchange مرة لكل يوزر لوجن
2) Client ticket granting server exchange مرة لكل نوع من الخدمات المطلوبه
3) Client application server exchange مرة لكل خدمه اليوزر طلبها لاي ابليكشن هايستخدمه

Four entities are used in the Kerberos system

1) Client workstation

وده اللي اليوزر بيخش من عليه علي السيستم

2) Authentication server(AS)

بيخزن عليه الباسوردات واي تفاعل من اليوزر مع السيستم زي ticket granting ticket اللي بتيجي من TG

3) Ticket granting ticket(TG)

المسئوله عن ticket وبتحط معاها timestamp عشان يحسب الوقت اللي اليوزر هايقعده داخل السيستم وبيكون داخل السيستم

الباكيت كلها بتبقي فيها time stamp , TG's ID, lifetime value , session key, ticket granting ticket

4) Application server(AP)

وده اللي بيقدم الخدمات بعد ما اليوزر بيخش علي السيستم ويعدي علي المراحل اللي فاتت

Public key authentication process

وده مابيطلبش من اليوزر انه يعمل share او يخزن اي باسورد داخل السيستم

بيستخدم key واحد للتشفير واكتر من key مختلفين بس ليهم علاقه ببعض لفك تشفير key ده